USAccess Program Definitions

Access control – the process of granting or denying requests to access physical facilities or areas, or to logical systems (e.g., computer networks or software applications). See also "logical access control system" and "physical access control system."

Authentication - the process of establishing an individual's identity and determining whether individual Federal employees or contractors are who they say they are.

Authorization - process of giving individuals access to specific areas or systems based on their rights for access and contingent on successful authentication.

Background Investigation – any one of various Federal investigations conducted by OPM, the FBI, or by Federal departments and agencies with delegated authority to conduct personnel security background investigations.

Biometric – a measurable physical characteristic used to recognize the identity of an individual. Examples include fingerprints and facial images. A biometric system uses biometric data for authentication purposes.

Contractor – see "Employee".

Employee – as defined in Executive Order (EO) 12968, "Employee" means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts on behalf of an agency as determined by the agency head. See also "Employee" as defined in title 5 U.S.C §2105.

e-QIP Tracking Number – Number assigned by e-QIP to each Form SF-85 application. For those Interior bureaus and offices using e-QIP, the tracking number must be written on the fingerprint card when it is submitted to OPM in order to bind the fingerprint card to the proper applicant.

FBI FP Check – National Criminal History Fingerprint check of the FBI fingerprint files. This check is an integral part of the NACI.

Identity Management System (IDMS) - one or more systems or applications that manage the identity verification, validation, and card issuance process. The IDMS software is used by PIV Registrars to enroll Applicants.

Identity-proofing – the process of providing identity source documents (e.g., driver's license, passport, birth certificate, etc.) to a registration authority, or the process of verifying an individual's information that he or she is that individual and no other. FIPS 201-1 requires that one of these documents be an original State or Federal Government-issued photo ID, and the other be from the approved set of identity documents listed on Form I-9.

Logical Access Control System (LACS) – protection mechanisms that limit users' access to information technology (IT) systems by restricting their form of access to those systems necessary to perform their job function. These LACS may be built into an operating system, application, or an added system.

National Agency Check (NAC) – The NAC is part of every NACI. Standard NACs are Security/Suitability Investigations Index, Defense Clearance and Investigation Index, FBI Name Check, and FBI National Criminal History Check.

USAccess Program Definitions

National Agency Check with Inquiries (NACI) – the basic and minimum investigation required of all Federal employees and contractors consisting of searches of the OPM Security/ Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation (FBI) Identification Division's name and fingerprint files, and other files or indices when necessary. A NACI also includes written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities).

Physical Access Control System (PACS) – protection mechanisms that limit users' access to physical facilities or areas within a facility necessary to perform their job function. These systems typically involve a combination of hardware and software (e.g., a card reader), and may involve human control (e.g., a security guard).

PIV-II Credential – a government-issued identity credential, referred to as a smart card, which contains a contact and contact-less chip. The Cardholder's facial image will be printed on the card along with other identifying information and security features that can be used to authenticate the user for physical access to federally controlled facilities. The card may include a PKI certificate, which controls logical access to federally controlled information systems.

Public Key Infrastructure (PKI) – A service that provides cryptographic keys needed to perform digital signature-based identity verification, and to protect communications and storage of sensitive data.

SF-87 - Fingerprint Chart for Federal employee(s) or applicant for Federal employment.

Submitting Office Identifier (SOI) – Number assigned by OPM to identify office that submitted the NACI request